Topology Vol. 4, pp. 109–127. Pergamon Press, 1965. Printed in Great Britain

SELF-EQUIVALENCES OF PSEUDO-PROJECTIVE PLANES†

PAUL OLUM‡

(*Received* 25 *January* 1965)

INTRODUCTION

LET X be a space with base point and let $\mathscr{E}(X)$ denote the group of homotopy classes of homotopy equivalences of X into itself, the group operation being composition; all maps and homotopies are required to leave the base point fixed. We shall call $\mathscr{E}(X)$ the "self-equivalence group" of X.

The group $\mathscr{E}(X)$ is a natural one to study, being, in a sense, the most general group of "symmetries up to homotopy" of the space X. Very little is known about this group in general (see, however, [1], [2, §6] and [13]) and we propose to examine it here in detail for some very elementary spaces, the pseudo-projective planes. A pseudo-projective plane of order q (q a positive integer), denoted P_q, is the space formed from the unit disk by the identification on S^1 (in polar coordinates): $(1, \theta) \equiv \left(1, \theta + \frac{2\pi}{q}\right)$; we take the point * represented by $(1, 0)$ as base point.

The problem of determining $\mathscr{E}(P_q)$ was proposed by J. H. C. Whitehead, presumably in connection with his study of simple homotopy type, especially simple homotopy type for lens spaces. Whitehead raised, in particular, the question of which automorphisms of $\pi_1(P_q)$ are realized by self-equivalences.

Our general results on the structure of $\mathscr{E}(P_q)$ are given in §§3–5 below; this structure turns out to be surprisingly rich and to be related to rather deep results and problems of algebraic number theory. As an application, we discuss in detail in §6 the possible orders of self-equivalences and the relationship of these orders to induced automorphisms of $\pi_1(P_q)$. It turns out that all automorphisms of $\pi_1(P_q)$ do occur and that the possible orders of the self-equivalences inducing a particular one depend strongly on number-theoretic properties of the automorphism; see Theorem 6.2.

In §7 we consider briefly a number of related matters, e.g. the group of "free" self-equivalences, explicit constructions of self-equivalences, etc. In a short appendix, §8, we

† This paper was originally intended for one of the issues dedicated to Arnold Shapiro, but it was unfortunately submitted too late for that. The author would like to record here his own deep affection and respect for Shapiro as well as his very great mathematical indebtedness to him.

‡ This work was done with the support of the National Science Foundation under grant NSF GP 2037.

prove a theorem (needed in the body of the paper) which shows how difference homomorphisms of cohomology are determined by obstructions.

I am indebted to several people for helpful conversations about the present work, among them James Ax, Peter Hilton, John Milnor and Alex Rosenberg. In particular, I have profited greatly from a number of talks with Ax about algebraic number theory.

We shall not consider here the problem of "simple" self-equivalences or, more generally, the determination of the torsion of a given element of $\mathcal{E}(P_q)$. The problem is an interesting one and we intend to discuss it in a subsequent paper.

§1. COHOMOLOGY INVARIANT OF A MAP

Let $a \epsilon \pi_1(P_q)$ be the element represented by the loop $r = 1$, $\theta = \dfrac{2\pi t}{q}$ where t runs from 0 to 1. Then $\pi_1(P_q)$ is clearly cyclic of order q, generated by a; we write π_1 for $\pi_1(P_q)$.

A map $f: P_q \to P_q$ induces $f_*: \pi_1 \to \pi_1$ with $f_*(a) = a^s$ for some integer s, $0 \leqq s < q$. We restrict ourselves to maps f which induce an automorphism of π_1 or, equivalently:

(1.1) We assume throughout that $(s, q) = 1$ where $f_*(a) = a^s$.

Ultimately we shall be interested only in self-equivalences and for these (1.1) must, of course, be satisfied.

We look now at the homomorphism of 2-dimensional cohomology induced by f. As coefficients we use the quotient $\Gamma_q = Z[\pi_1]/I$, where $Z[\pi_1]$ is the group-ring of π_1 over the integers and I is the ideal generated by $(1 + a + \ldots + a^{q-1})$; Γ_q is, effectively, $\pi_2(P_q)$; see (2.10) below. We write an element of $Z[\pi_1]$ as $\sum n_i a^i$, where the n_i are integers and i runs from 0 to $q-1$, and we denote by $\gamma = \{\sum n_i a^i\}$ its class in Γ_q.

Sine π_1 operates on $Z[\pi_1]$, and hence on Γ_q, by the ring multiplication, we shall take Γ_q as a local coefficient group in P_q. The mapping f induces then a homomorphism

$$f^*: H^2(P_q; \Gamma_q) \to H^2(P_q; \Gamma_q^s) \tag{1.2}$$

where Γ_q^s denotes the local group in P_q induced from Γ_q by f; thus, $\Gamma^s = \Gamma_q^s$ as a group, but, if the operation of π_1 is indicated by $a^i\gamma$ in Γ_q and $a^i \cdot \gamma$ in Γ_q^s, then $a^i \cdot \gamma = a^{is}\gamma$.

In order to relate the two coefficient systems we introduce an automorphism θ_s of the ring Γ_q defined by

$$\theta_s\{\textstyle\sum n_i a^i\} = \{\sum n_i a^{is}\}. \tag{1.3}$$

We may regard θ_s as giving an isomorphism of local groups: $\Gamma_q \to \Gamma_q^s$ since it clearly commutes with the operation of π_1 here. Hence it induces an isomorphism

$$\theta_{s*}: H^2(P_q, \Gamma_q) \to H^2(P_q, \Gamma_q^s). \tag{1.4}$$

Note that an element $\gamma \epsilon \Gamma_q$ operates by multiplication to give an endomorphism of Γ_q and also of Γ_q^s, taken as local groups in P_q, and hence endomorphisms of $H^2(P_q; \Gamma_q)$ and $H^2(P_q; \Gamma_q^s)$, which thus become Γ_q-modules. For h in $H^2(P_q; \Gamma_q)$ or in $H^2(P_q; \Gamma_q^s)$ we write the result of this operation as γh. It is then immediate from (1.2)-(1.4) that

$$f^*(\gamma h) = \gamma f^*(h) \tag{1.5}$$

$$\theta_{s*}(\gamma h) = \theta_s(\gamma)\theta_{s*}(h). \tag{1.6}$$

For the sake of explicitness in a later construction (see (7.5)), we suppose P_q given a fixed triangulation, with vertices ordered, and we let σ_2 be a chosen 2-simplex with its leading vertex at the base point *. Every element of $H^2(P_q; \Gamma_q)$ is uniquely represented by a cocycle of the form $\gamma\sigma^2$, $\gamma\epsilon\Gamma_q$, where σ^2 is the integral cochain with value 1 on σ_2, value 0 on all other simplexes; there are no non-trivial coboundaries in this representation. This correspondence gives us then an explicit isomorphism of Γ_q-modules:

$$H^2(P_q; \Gamma_q) \approx \Gamma_q. \tag{1.7}$$

We use 1 to denote the unit element of Γ_q and also to denote the corresponding element of $H^2(P_q; \Gamma_q)$ under (1.7). Then θ_{s*} (1) generates the Γ_q-module $H^2(P_q; \Gamma_q^s)$.

Definition 1.8. Given $f: P_q \to P_q$ with $f_*(a) = a^s$, we associate with it a *cohomology invariant* $\gamma_f \epsilon \Gamma_q$ defined by $f^*(1) = \gamma_f \theta_{s*}(1)$.

It is clear from (1.5) that γ_f determines f^* completely. The invariant γ_f will be our principal tool in studying the mapping f.

Definition 1.9. We define a ring homomorphism

$$A : \Gamma_q \to Z_q$$

where Z_q is the integers mod q, by setting $A\{\sum n_i a^i\} = \sum n_i \pmod q$; we shall call $A(\gamma)$ the augmentation of γ.

We assert now the following four properties of γ_f:

$$f_*(a) = a^{A(\gamma_f)}; \text{ hence, by (1.1), } (A(\gamma_f), q) = 1. \tag{1.10}$$

$$f \cong g \text{ rel.* if and only if } \gamma_f = \gamma_g. \tag{1.11}$$

$$\text{Given } \gamma \epsilon \Gamma_q \text{ with } (A(\gamma), q) = 1, \text{ there is an } f: P_q \to P_q \text{ such that } \gamma_f = \gamma. \tag{1.12}$$

$$\gamma_{fg} = \gamma_f \theta_s(\gamma_g) \text{ where } s = A(\gamma_f). \tag{1.13}$$

For the proof of (1.13), suppose $g_*(a) = a^t$. The θ_s of (1.3) may be regarded also as giving an isomorphism of local groups $\Gamma_q^t \to \Gamma_q^{st}$ and a resulting isomorphism of cohomology. It is clear that $g^*\theta_{s*} = \theta_{s*}g^*: H^2(P_q; \Gamma_q) \to H^2(P_q; \Gamma_q^{st})$. Using this and (1.5) and (1.6) we get at once $g^*f^*(1) = \gamma_f \theta_s(\gamma_g)\theta_{st*}(1)$.

The proofs of (1.10), (1.11), (1.12) will be given at the end of §2.

§2. OBSTRUCTION INVARIANT OF A MAP

Another way of associating an algebraic invariant with a map is through obstruction theory. If f and g are homotopic in dimension 1, i.e. if $f_*(a) = g_*(a) = a^s$, then $\mathcal{O}^2(f, g)$ is defined. It is an element of $H^2(P_q; \pi_2^s)$, where $\pi_2(P_q)$ is taken naturally as a local group in P_q and π_2^s denotes the local group induced from this by $f_*: \pi_1 \to \pi_1$. We recall the following well-known properties; see [10]:

$$f \cong g \text{ rel.* if and only if } f_* = g_*: \pi_1 \to \pi_1 \text{ and } \mathcal{O}^2(f, g) = 0. \tag{2.1}$$

(2.2) Given $f: P_q \to P_q$ and $h \epsilon H^2(P_q; \pi_2^s)$, then there is a $g: P_q \to P_q$ such that $\mathcal{O}^2(f, g) = h$.

(2.3) If f, f', f'' are all homotopic in dimension 1, then $\mathcal{O}^2(f, f'') = \mathcal{O}^2(f, f') + \mathcal{O}^2(f', f'')$.

For each integer s, with $0 < s < q$ and $(s, q) = 1$, we can define in a very simple way a particular map $f_s: P_q \to P_q$ such that $f_{s*}(a) = a^s$, as follows: we map the unit disk into itself by $(r, 0) \to (r, s\theta)$ and then pass to f_s by the identification on S^1.

Definition 2.4. Given $f: P_q \to P_q$ with $f_*(a) = a^s$, we associate with it the pair (s, h) where $h = \mathcal{O}^2(f, f_s)$; call (s, h) the *obstruction invariant* of f.

From (2.1)–(2.3) we get at once the following:

(2.5) If f and f' have obstruction invariants (s, h) and (s', h'), then $f \cong f'$ rel.* if and only if $s = s'$ and $h = h'$.

(2.6) Given $h \epsilon H^2(P_q; \pi_2^s)$, there is an $f: P_q \to P_q$ with obstruction invariant (s, h).

Now we look at the relationship between these obstruction invariants and the γ_f of (1.8). For this we define a homomorphism of local groups:

$$\psi : \pi_2(P_q) \to \Gamma_q \tag{2.7}$$

as follows. Given any $\alpha \epsilon \pi_2(P_q)$, we let $\phi: S^2 \to P_q$ be a (base-point preserving) map of an oriented 2-sphere into P_q representing α and we form $\phi^*(1) \epsilon H^2(S^2; \Gamma_q)$, where $1 \epsilon H^2(P_q; \Gamma_q)$ is as in (1.8). Then $(\phi^*(1))(h_2)$ is an element of Γ_q, where h_2 is the generator of $H_2(S^2; Z)$ specified by the orientation; we define $\psi(\alpha)$ to be this element. It is easily seen that ψ commutes with the operation of π_1.

The ψ of (2.7) may also be regarded then as a homomorphism of the local groups: $\pi_2^s \to \Gamma_q^s$ and as such it induces

$$\psi_* : H^2(P_q; \pi_2^s) \to H^2(P_q; \Gamma_q^s). \tag{2.8}$$

We have now the following lemma, the proof of which (under much more general circumstances) will be given in the appendix, §8.

LEMMA 2.9. *If $f, g: P_q \to P_q$ satisfy $f_*(a) = g_*(a) = a_i^s$, then $f^*(1) - g^*(1) = \psi_*(\mathcal{O}^2(f, g))$.*

The structure of $\pi_2(P_q)$ is easily determined; every element can be written in the form $\sum n_i a^i \alpha_0$, summed from 0 to $q-1$, where $\alpha_0 \epsilon \pi_2(P_q)$ is a suitably chosen generator, and $\sum n_i a^i \alpha_0 = 0$ if and only if $n_i = n_0$ for all i. Hence, we have

(2.10) We may write the elements of $\pi_2(P_q)$ uniquely in the form $\eta\alpha_0$, with $\eta \epsilon \Gamma_q$, and the correspondence $\eta\alpha_0 \leftrightarrow \eta$ gives an isomorphism: $\pi_2(P_q) \approx \Gamma_q$ as local groups in P_q.

$H^2(P_q; \pi_2^s)$ is isomorphic to Γ_q then, each cohomology class being uniquely represented by a cocycle of the form $(\eta\alpha_0)\sigma^2$, where σ^2 is as in §1. The computation of ψ_* is now straightforward and elementary and, with the appropriate choice of α_0, yields the following result.

LEMMA 2.11. *Let $h \epsilon H^2(P_q; \pi_2^s)$ be represented by $(\eta\alpha_0)\sigma^2$. Then $\psi_*(h) = \{1 - a\}\, \eta\theta_{s*}(1)$.*

An examination of this formula for ψ_* yields the following corollary.

COROLLARY 2.12. *ψ_* is a monomorphism. The image of ψ_* is the subgroup of $H^2(P_q; \Gamma_q^s$ consisting of all elements $\gamma\theta_{s*}(1)$ for which $A(\gamma) = 0$.*

The cohomology invariant γ_{f_s} of the special map f_s defined above is easily computed from the definition and is just $\{s\}\epsilon\Gamma_q$. Lemmas (2.9) and (2.11) then give us:

COROLLARY 2.13. *If $f: P_q \to P_q$ has obstruction invariant (s, h), where $h = \mathcal{O}^2(f, f_s)$ is represented by $(\eta\alpha_0)\sigma^2$, then*

$$\gamma_f = \{s\} + \{1 - a\}\eta.$$

We can now prove the properties (1.10)–(1.12) at the end of §1.

For (1.10): Let $f_*(a) = a^s$. Since $A(\{1 - a\}\eta) = 0$, we get from (2.13) that $A(\gamma_f) \equiv s \pmod q$.

For (1.11): Since ψ_* is a monomorphism by (2.12), (1.11) follows at once from (2.1), (1.10) and (2.9).

For (1.12): Choose the integer s, $0 < s < q$, so that $A(\gamma) \equiv s \pmod q$. By (2.12), then, there is an $h\epsilon H^2(P_q; \pi_2^s)$ such that $\psi_*(h) = (\gamma - \{s\})\,\theta_{s*}(1)$. By (2.6), there is an f with obstruction invariant (s, h) and, by Lemma (2.11) and Corollary (2.13), $\gamma_f = \{s\} + (\gamma - \{s\}) = \gamma$.

§3. THE DETERMINATION OF $\mathcal{E}(P_q)$

We shall give the determination of $\mathcal{E}(P_q)$ here (in two ways) in Theorems (3.4) and (3.5); the algebraic description provided by Theorem (3.5) is the principal one.

The ring Γ_q was defined above as the quotient of $Z[\pi_1]$ over the ideal $I = (1 + a + \cdots + a^{q-1})$. This is canonically isomorphic to the quotient of the integral polynomial ring $Z[x]$ over the ideal $(1 + x + \ldots + x^{q-1})$ and henceforth we shall identify these two interpretations of Γ_q; generally we shall take Γ_q in the latter sense and represent its elements as $\gamma = \{f(x)\}$, $f(x)\epsilon Z[x]$. With this interpretation, $\theta_s\{\sum n_i x^i\} = \{\sum n_i x^{is}\}$ and $A\{\sum n_i x^i\} = \sum n_i \pmod q$.

Definition 3.1. Let U_q denote the group of units in Γ_q and let U_q^1 denote the subgroup of U_q consisting of units of augmentation $+1$.

Definition 3.2. With multiplication in U_q denoted by juxtaposition, let E_q be the group whose elements are those of U_q but with a multiplication $\circ$ defined by

$$\gamma_1 \circ \gamma_2 = \gamma_1 \theta_s(\gamma_2)$$

where $s = A(\gamma_1)$. E_q is non-abelian for $q > 2$, since $-1 \circ \{x\} \neq \{x\} \circ -1$. Note that the two multiplications coincide on U_q^1 so that U_q^1 may also be regarded as a subgroup of E_q.

Definition 3.3. Let Z_q^* denote the multiplicative group of reduced residues mod q; it is canonically isomorphic to, and may be identified with, the group Aut π_1 of automorphisms of π_1. Note that the augmentation A gives us group homomorphisms (which we shall again denote by A): $U_q \to Z_q^*$ and $E_q \to Z_q^*$.

Now if we denote by $\{f\}$ the class of the self-equivalence f in $\mathcal{E}(P_q)$, properties (1.10)–(1.13) give us the theorem:

THEOREM 3.4. *The map $\kappa: \mathcal{E}(P_q) \to E_q$ defined by $\kappa\{f\} = \gamma_f$ is an isomorphism. Furthermore $f_*: \pi_1 \to \pi_1$ is given by $f_*(a) = a^{A(\gamma_f)}$.*

A somewhat more perspicuous algebraic description of $\mathcal{E}(P_q)$ is given by combining Theorem (3.4) with the following theorem whose verification is immediate.

THEOREM 3.5. *The group E_q is a split extension* (see [3, p. 299]):

$$1 \to U_q^1 \xrightarrow{i} E_q \xrightarrow{A} Z_q^* \to 1$$

where *i is injection and A augmentation and where the result of the operation of $s \epsilon Z_q^*$ on $u \epsilon U_q^1$ is $\theta_s(u)$. A splitting is provided by $B: Z_q^* \to E_q$ defined by*†

$$B(s) = \{1 + x + \cdots + x^{s-1}\}.$$

Remark 3.6. The groups Z_q^* and U_q^1 are both abelian and we may define the semi-direct product $U_q^1 \times Z_q^*$ by the commutation rule $s \times u = \theta_s(u) \times s$, where $u \epsilon U_q^1$, $s \epsilon Z_q^*$. Then any splitting B of the exact sequence of Theorem (3.5) (such as the one given) provides us with an explicit isomorphism $\mu_B: \mathcal{E}(P_q) \approx U_q^1 \times Z_q^*$.

Remark 3.7. Probably the nicest and simplest way to formulate our result above is the following. The projection $\rho: Z[\pi_1] \to \Gamma_q$ is easily seen to map the group of units in $Z[\pi_1]$ isomorphically onto the units of augmentation ± 1 in Γ_q. We may therefore identify U_q^1 instead as the group of units of $Z[\pi_1]$ whose augmentation (in the obvious sense) is $+1$. Theorems 3.4 and 3.5 then give us:

The self-equivalence group $\mathcal{E}(P_q)$ is a split extension:

$$1 \to U_q^1 \xrightarrow{j} \mathcal{E}(P_q) \xrightarrow{\alpha} \mathrm{Aut}(\pi_1) \to 1 \tag{3.8}$$

where $\alpha\{f\} = f_*: \pi_1 \to \pi_1$, $j(u) = \{f\}$ such that $\gamma_f = u$, and $\mathrm{Aut}(\pi_1)$ operates in the obvious way on $Z[\pi_1]$ and hence on U_q^1.

We shall find it more satisfactory, however, to continue to regard U_q^1 as a subgroup of U_q in Γ_q and to take Γ_q as $Z[x]/(1 + x + \cdots + x^{q-1})$; the reason for this, as we shall see below in §5, is the availability of certain "standard units" in U_q.

§4. THE STRUCTURE OF THE GROUP OF UNITS

In view of the results given in §3, we can study the detailed algebraic structure of the self-equivalence group $\mathcal{E}(P_q)$ by examining the abelian groups Z_q^* and U_q^1 and the operation of Z_q^* on U_q^1.

The group Z_q^* is, of course, very well known. It is a finite group with $\phi(q)$ elements, where ϕ is Euler's function; for details of its structure see [15, Ch. 6].

In studying U_q^1, it will be convenient to consider the abelian group U_q of all units in Γ_q and to get the desired information about U_q^1 as a corollary.

THEOREM 4.1. *If we denote*

$$\rho_q = \textit{rank of } U_q \tag{4.2}$$

† We shall regularly use the same symbol for an element of Z_q^* and a representative integer, generally between 0 and q, of this residue class; no ambiguity will arise.

then ρ_q is equal to the number of integers between 1 and $q/2$ which do not divide q. The torsion subgroup of U_q consists of the trivial units $\pm\{x^i\}$, $i = 0, 1, \ldots, q-1$.

COROLLARY 4.3. *The rank of U_q^1 is also given by the ρ_q of* (4.2). *The torsion subgroup of U_q^1 is the cyclic group of order q generated by $\{x\}$.*

Proof. The corollary is immediate from the theorem since U_q^1 is a subgroup of U_q of finite index $\phi(q)$.

For q a prime, the theorem is essentially Dirichlet's theorem on the units of $Z[\zeta]$ where ζ is a primitive root of unity. For arbitrary q we can reduce the determination of ρ_q to an application of Dirichlet's theorem by the following argument.

We look at the ring homomorphism

$$\lambda : \Gamma_q = \frac{Z[x]}{(1 + x + \cdots + x^{q-1})} \to \sum_{\substack{h|q \\ h \neq 1}} Z[\zeta_h] \tag{4.3}$$

which will play an essential role in much of our work. Here, for each h, ζ_h is a primitive h-th root of unity and λ is defined by $\lambda\{f(x)\} = \sum f(\zeta_h)$ for $f(x) \in Z[x]$.

Let $\Phi_h(x)$ denote the irreducible cyclotomic polynomial with ζ_h as a root. If we were using rational coefficients Q instead of integers Z, then, regarding $Q[\zeta_h]$ as $Q[x]/(\Phi_h(x))$ and using the Chinese remainder theorem, λ would clearly be an isomorphism. For the case of integer coefficients, however, precisely the same argument proves (i) that λ is a monomorphism and (ii) that there exists an integer N such that $(N) \subset$ image λ, where (N) is the ideal in $\sum Z[\zeta_h]$ consisting of all elements divisible by N.

If we now consider the natural projection

$$\pi : \sum Z[\zeta_h] \to \sum Z[\zeta_h]/(N) \tag{4.4}$$

the ring on the right is finite; hence the multiplicative group of units in this ring has finite order, say n. Then, for any unit $v \in \sum Z[\zeta_h]$, $\pi v^n = 1$; therefore $v^n - 1 \in (N)$ and it follows that v^n is in image λ.

Since λ is a monomorphism, we deduce that the rank ρ_q of the unit group U_q of Γ_q is the same as that of the unit group of $\sum Z[\zeta_h]$. But, by Dirichlet's theorem [8, Theorems 14.5 and 8.6], the rank of the units in $Z[\zeta_h]$ is $\frac{1}{2}\phi(h) - 1$ for $h \neq 2$ and 0 for $h = 2$. Hence

$$\rho_q = \sum_{\substack{h|q \\ h>2}} (\tfrac{1}{2}\phi(h) - 1). \tag{4.5}$$

Clearly $\sum \phi(h)$ here is $q - 1$ for q odd, $q - 2$ for q even. The assertion of the theorem about ρ_q then follows at once from (4.5).

It remains to examine the torsion subgroup of U_q. Given an element of finite order in U_q we can represent it by a polynomial $f(x) \in Z[x]$ of degree less than q such that $f(1) = b$, $0 < b < q$.

Then, for any primitive h-th root of unity, with $h|q$ but $h \neq 1$, $f(\zeta_h)$ is a root of unity in $Z[\zeta_h]$; see (4.3). But the roots of unity in $Z[\zeta_h]$ clearly form a cyclic group of order k, where (since $h|k$ and $\phi(k)|\phi(h)$) $k = h$ for h even and $k = 2h$ for h odd; thus the group is generated by ζ_h, h even, and $-\zeta_h$, h odd.

If ζ is a primitive q-th root of unity then, we have

$$f(\zeta^i) = \epsilon_i \zeta^{ij_i} \qquad i = 1, 2, \ldots, q-1$$

where $\epsilon_i = +1$ or -1 and $j_i \epsilon Z$. Now† we may write, all sums being taken from 0 to $q-1$:

$$f(x) = \sum_k c_k x^k \qquad c_k \epsilon Z$$

$$\sum_k c_k \zeta^{ik} = f(\zeta^i) = \begin{cases} \epsilon_i \zeta^{ij_i} & i = 1, 2, \ldots, q-1 \\ b & i = 0 \end{cases} \tag{4.6}$$

$$\sum_k c_k \sum_i \zeta^{ik-im} = \sum_i \epsilon_i \zeta^{ij_i - im} + (b-1)$$

for $m = 0, 1, \ldots, q-1$, where we have for convenience introduced $\epsilon_0 = +1$. Since $\sum \zeta^{ik-im}$ is 0 for $k \neq m$ and q for $k = m$, we get

$$qc_m - (b-1) = \sum_i \epsilon_i \zeta^{ij_i - im}.$$

Then, since $c_m \epsilon Z$ and $0 < b < q$, we see from taking absolute values that $c_m \neq 0$ implies $c_m = 1$. Thus we get

$$f(x) = x^{m_1} + x^{m_2} + \cdots + x^{m_b} \qquad 0 \leqq m_1 < m_2 < \cdots < m_b < q. \tag{4.7}$$

Now from this we can compute

$$\sum_i f(\zeta^i) f(\zeta^{-i}) = \sum_i \sum_{j,k} \zeta^{im_j} \zeta^{-im_k} = qb$$

where i runs from 0 to $q-1$ and j, k run from 1 to b; the final equality comes from interchanging order and using again that

$$\sum_i \zeta^{i(m_j - m_k)} \text{ is } 0 \text{ for } m_j \neq m_k \text{ and } q \text{ for } m_j = m_k.$$

On the other hand, from (4.6),

$$\sum_i f(\zeta^i) f(\zeta^{-i}) = q - 1 + b^2.$$

Hence $qb = q - 1 + b^2$ and $b = 1$ or $b = q-1$. We insert these in (4.7). The first gives us $f(x) = x^{m_1}$. From the second we get that, for some m, $\{f(x)\} = -\{x^m\}$. This completes the proof.

§5. STANDARD UNITS AND THE ALGEBRAIC STRUCTURE OF $\mathscr{E}(P_q)$

Further knowledge of the structure of $\mathscr{E}(P_q)$ depends upon information about the operation of Z_q^* on U_q^1. We could explicitly describe this operation if we could get a complete set of independent generators for the free part of U_q^1. But this is, in general, an exceedingly difficult matter. Even for the special case where q is a prime p this reduces (using (4.3)) to the well-known unsolved problem of producing a basis for the units in $Z[\zeta_p]$.

We can, however, produce a particular very useful set of independent units, which is in some cases large enough, and we shall look at this now. Once again we consider first the full group U_q of units in Γ_q.

Definition 5.1. We shall call the units

$$e_i = \left\{\frac{1-x^i}{1-x}\right\} = \{1 + x + \cdots + x^{i-1}\} \qquad (i, q) = 1$$

† The argument which follows was given to me by James Ax.

standard units in U_q. (To see that e_i is a unit, let k be an integer such that $ik \equiv 1 \pmod q$; then $e_i\{(1-x^{ik})/(1-x^i)\} = 1$ in Γ_q.)

We note that

$$e_{q-i} = \left\{\frac{1-x^{q-i}}{1-x}\right\} = -\{x^{q-i}\}e_i \tag{5.2}$$

so that (to within trivial units) we may confine attention to the e_i for which $1 < i < q/2$.

Definition 5.3. An element $r \epsilon Z_q^*$ is called *primitive* if it generates Z_q^*. We shall call r *semi-primitive* if r and -1 together generate Z_q^*; semi-primitive includes primitive then. There exists a primitive element in Z_q^* if and only if $q = 4$, p^α or $2p^\alpha$ where p is an odd prime and α a non-negative integer; see [15, p. 121]. Using [15, Ch. VI, §§6, 7] one can show that there is a semi-primitive element in Z_q^* if and only if q has one of the following forms, where p and w are odd primes and α and β are non-negative integers: 2^α; $2^j p^\alpha$ where $j = 0, 1, 2$; $2^k p^\alpha w^\beta$ where $k = 0, 1$ and $(p^{\alpha-1}(p-1),\ w^{\beta-1}(w-1)) = 2$. We omit the proof. The only $q \leqq 50$ for which Z_q^* does not contain a semi-primitive element are 24, 40 and 48.

In case there exists a semi-primitive r in Z_q^*, we may consider another set of units of U_q, essentially equivalent to the standard set defined above, as follows.

Definition 5.4. Let $r \epsilon Z_q^*$ be a fixed semi-primitive element and let

$$\epsilon_i = \left\{\frac{1-x^{r^{i+1}}}{1-x^{r^i}}\right\} = \{1 + x^{r^i} + \cdots + x^{(r-1)r^i}\} \tag{5.5}$$

for any i. Note that, if r is in fact primitive, $r^{\frac{1}{2}\phi(q)} = -1$; thus, for $j = \frac{1}{2}\phi(q) + i$, we have $\epsilon_j = \theta_{-1}(\epsilon_i)$ if r is primitive, and $\epsilon_j = \epsilon_i$ if r is not primitive. Furthermore (whether or not r is primitive)

$$\theta_{-1}(\epsilon_i) = \left\{\frac{1-x^{-r^{i+1}}}{1-x^{-r^i}}\right\} = \{x^{r^i(1-r)}\}\epsilon_i. \tag{5.6}$$

Finally, we see that

$$\epsilon_0 \epsilon_1 \cdots \epsilon_{\frac{1}{2}\phi(q)-1} = \begin{cases} -x^{-1} & r \text{ primitive} \\ 1 & r \text{ not primitive.} \end{cases} \tag{5.7}$$

Consequently (to within trivial units) we may confine attention to the ϵ_i for $i = 0, 1, \ldots, \frac{1}{2}\phi(q) - 2$. Note that all of the ϵ_i have the same augmentation: $A(\epsilon_i) = r$.

Definition 5.8. Let $\overline{U}_q$ denote the subgroup of U_q generated by the standard units e_i together with the trivial units. It is clear from the above that (where defined) the ϵ_i, with the trivial units, generate precisely the same subgroup. We shall call $\overline{U}_q$ the *standard subgroup* of U_q.

We have now the following theorem about these units, which is a consequence of classical results in algebraic number theory.

THEOREM 5.9. *We consider the* $\frac{1}{2}\phi(q) - 1$ *elements* e_i *for* $(i, q) = 1$ *and* $1 < i < q/2$ *and also (where defined) the elements* ϵ_i *for a fixed semi-primitive* r *and* $i = 0, 1, \ldots, \frac{1}{2}\phi(q) - 2$.

(a) *The standard subgroup* $\overline{U}_q$ *has rank* $\frac{1}{2}\phi(q) - 1$. *Hence the* e_i*'s are an independent set of units in* U_q *and so are the* ϵ_i*'s.*

(b) *If q is a prime, $\overline{U}_q$ has finite index in U_q.*

(c) *If q is a prime less than 23, or if $q = 8$ or 9, $\overline{U}_q = U_q$.* (It is not true that $\overline{U}_q = U_q$ for all prime q; see Remark 5.22 below.)

(d) *U_{10} is generated by the independent units $e_3 = \{1 + x + x^2\}$ and $f = \{1 - x^2 - x^3 - x^7 - x^8\}$ together with the trivial units.* (Note: $f^{-1} = \{x + x^4 - x^5 + x^6 + x^9\}$).

Before we give the proof of this theorem we shall look at its consequences for the group $\mathscr{E}(P_q)$. It will be most convenient here to assume that a particular splitting B of the exact sequence of Theorem (3.5) is chosen so that we have a definite isomorphism onto the semi-direct product:

$$\mu_B : \mathscr{E}(P_q) \approx U_q^1 \times Z_q^* \tag{5.10}$$

as in Remark 3.6.

We may set

$$\overline{U}_q^1 = \overline{U}_q \cap U_q^1. \tag{5.11}$$

It is clear that $\overline{U}_q$ and U_q^1, and hence also $\overline{U}_q^1$, admit the operator θ_s for all $s \epsilon Z_q^*$; in particular, $\theta_s(e_i) = e_{is} e_s^{-1}$. It is therefore meaningful to regard $\overline{U}_q^1 \times Z_q^*$ as a subgroup of $U_q^1 \times Z_q^*$.

It is somewhat cumbersome (although quite possible) to give explicitly a basis for the free part of $\overline{U}_q^1$ for general q. However, when there exists a semi-primitive element in Z_q^* this can be done very simply, as follows.

Definition 5.12. Let r be semi-primitive and let ϵ_i be as in (5.5). Choose a fixed m, $0 < m < q$, so that $2m \equiv 1 - r \pmod{q}$; this is always possible, uniquely if q is odd, with two choices if q is even. Then set

$$b_i = \{x^{m(1-r)r^i}\} \epsilon_i \epsilon_{i+1}^{-1} \qquad \text{in } \overline{U}_q^1 \tag{5.13}$$

for all i. (The factor $\{x^{m(1-r)r^i}\}$ is not essential; it is put in because it simplifies considerably formulas (5.14), (5.15) and (5.18) below; see also Remark 6.10.)

The relations

$$b_{\frac{1}{2}\phi(q)+i} = b_i \tag{5.14}$$

$$b_0 b_1 b_2 \cdots b_{\frac{1}{2}\phi(q)-1} = 1 \tag{5.15}$$

always hold and are easily checked from (5.5)–(5.7) and the definition of m.

We have now, as a corollary of Theorem (5.9):

THEOREM 5.16. (a) *If q is a prime, $\overline{U}_q^1 \times Z_q^*$ has finite index in $U_q^1 \times Z_q^*$. If q is a prime less than 23 or if $q = 8$ or 9, it is the full group.* (*See also Remark* 5.22.)

(b) *If $r \epsilon Z_q^*$ is semi-primitive, the elements b_i of* (5.13) *for $i = 0, 1, \ldots, \frac{1}{2}\phi(q) - 2$ are independent and, together with $\{x\}$, generate $\overline{U}_q^1$. Furthermore, the commutation rule $s \times u = \theta_s(u) \times s$ of $\overline{U}_q^1 \times Z_q^*$ (see* (3.6)) *is given for all s by*

$$\theta_{r^j}(b_i) = b_{i+j} \qquad \text{all } i, j \tag{5.17}$$

$$\theta_{-1}(b_i) = b_i \qquad \text{all } i \tag{5.18}$$

and relations (5.14) *and* (5.15).

(c) U_{10}^1 *is generated by* $c_1 = -\{x^8\}e_3^2$, $c_2 = \{x^4\}e_3 f$ *and* $\{x\}$; *see Theorem* (5.9(d)). Also $\theta_3(c_1) = c_1^{-1}$, $\theta_3(c_2) = c_2^{-1}$.

Thus, for $q \leqq 11$ or $q = 13, 17, 19$, we have a completely explicit description of the algebraic structure of the self-equivalence group $\mathcal{E}(P_q)$.

Proof of Theorem 5.16. Part (a) is clear from (b) and (c) of Theorem (5.9).

For part (b), the independence of the b_i's is an easy consequence of the independence of the ϵ_i's (Theorem 5.9 (a)) together with (5.7). To see that the b_i's and $\{x\}$ generate $\overline{U}_q^1$, it is enough to show that they generate all elements $\pm \epsilon_0^{n_0}\epsilon_1^{n_1} \cdots \epsilon_k^{n_k}$ where $k = \frac{1}{2}\phi(q) - 2$, $\sum n_i = \frac{1}{2}\phi(q)$ and the sign is plus if r is not primitive, minus if it is. We can rewrite such an element, omitting trivial factors $\{x^j\}$,

$$\pm b_0^{n_0-1} b_1^{n_0+n_1-2} \cdots b_k^{\Sigma n_i - k - 1} \epsilon_0 \epsilon_1 \cdots \epsilon_{k+1}$$

and the desired result follows at once from (5.7). The formulas (5.17) and (5.18) are immediate from (5.6), (5.13) and the definition of m.

Part (c) follows at once from Theorem (5.9(d)) and the formulas $\theta_3(e_3) = -\{x^9\}e_3^{-1}$ and $\theta_3(f) = -\{x^5\}f^{-1}$, which are given by an elementary computation.

Proof of Theorem 5.9. For part (a) we use a theorem proved by Franz in [4, pp. 251–254]. He showed that if

$$\prod_{\substack{-q/2 < i < q/2 \\ (i,q)=1}} (1 - \zeta_h^i)^{a_i} = 1 \tag{5.19}$$

for every $h(\neq 1)$ which divides q, where ζ_h is a primitive h-th root of unity and the a_i are integers satisfying $a_{-i} = a_i$ and $\sum a_i = 0$, then $a_i = 0$ for all i. Since $(1 - \zeta_h^{-i})^{2q} = (1 - \zeta_h^i)^{2q}$, we see (by raising both sides to the 4 q-th power) that Franz's result is equivalent to the following. If

$$\prod_{\substack{1 \leqq i < q \\ (i,q)=1}} (1 - \zeta_h^i)^{a_i} = 1 \tag{5.20}$$

for every $h(\neq 1)$ which divides q, and $\sum a_i = 0$, then each $a_i = 0$.

Now suppose there are integers n_i such that

$$\prod_{1 < i < q/2} e_i^{n_i} = 1 \qquad \text{in } \Gamma.$$

Then, using the homomorphism λ of (4.3), it follows that for h/q, $h \neq 1$,

$$(1 - \zeta_h)^{-\Sigma n_i} \prod_{\substack{1 < i < q/2 \\ (i,q)=1}} (1 - \zeta_h^i)^{n_i} = 0$$

and therefore, by (5.20), each $n_i = 0$. Hence the e_i's are independent. It follows that the rank of $\overline{U}_q$ is $\frac{1}{2}\phi(q) - 1$ and that the ϵ_i's are independent.

If q is a prime, then, by Theorem (4.1), rank $U_q = \frac{1}{2}\phi(q) - 1 = \text{rank } \overline{U}_q$ and (b) follows.

For (c), with q a prime, we consider the λ of (4.3) again. It gives an isomorphism of U_q onto the units of $Z[\zeta_q]$ and this isomorphism maps $\overline{U}_q$ onto the subgroup of units generated by the "cyclotomic" units $(1 - \zeta_q^i)/(1 - \zeta_q)$ and the roots of unity $\pm \zeta_q$. The index of

this subgroup is known to be the second factor h_2 of the class number of the cyclotomic field $Q(\zeta_q)$ or, equivalently, the class number of the real subfield $Q(\zeta_q + \zeta_q^{-1})$, where Q = rationals; see [5, p. 171] and [16, §207, p. 759]. Now, if q is a prime less than 23, it is known that $h_2 = 1$; see [14, p. 568] and for details, [6, p. 472], [18], and [9, p. 296]. Consequently, for prime $q < 23$, $\overline{U}_q = U_q$.

If q is not a prime, we may consider

$$\lambda_q : \Gamma_q \to Z[\zeta_q] \tag{5.21}$$

i.e. the projection onto the first summand in (4.3). $\lambda_q(\overline{U}_q)$ is, as before, the subgroup of units generated by the cyclotomic units and roots of unity. If $q = 8$ or 9, this subgroup is the full group of units in $Z[\zeta_q]$; for $q = 8$, this is directly given by [16, §217, p. 794 and §207, p. 759]; for $q = 9$, the index of the subgroup is the second factor h_2 of the class number again ([5, p. 171] and [16, p. 759]) and this is 1 [17, p. 269].

Thus, for $q = 8$ or 9, we may write any $u \epsilon U_q$ as $u = v\bar{u}$ where $\bar{u} \epsilon \overline{U}_q$ and $\lambda_q(v) = 1$. But since the λ of (4.3) is a monomorphism and since the units in $Z[\zeta_q]$ for $q < 5$ are of finite order, it follows that v has finite order. Hence, by Theorem (4.1) and definition 5.8, $v \epsilon \overline{U}_q$ and, therefore, $U_q = \overline{U}_q$. This completes the proof of (c).

For (d), we look at (4.3) and (5.21) with $q = 10$. The units of $Z[\zeta_{10}]$ are generated by ζ_{10} and $1 - \zeta_{10}$. This follows at once from the fact that $-\zeta_{10}$ is a primitive 5-th root of unity and we know, from part (c), that $-\zeta_5$ and $1 + \zeta_5$ generate $Z[\zeta_5]$.

Now $\lambda_{10}(\overline{U}_{10})$ of (5.21) is generated by ζ_{10} and $1 + \zeta_{10} + \zeta_{10}^2 = \zeta_{10}^{-3}(1 - \zeta_{10})^{-2}$, i.e. by ζ_{10} and $(1 - \zeta_{10})^2$. Furthermore, there is no $u \epsilon U_{10}$ such that $\lambda_{10}(u) = 1 - \zeta_{10}$; to see this, we represent u by a polynomial $f(x)$ of degree less than 9; elementary direct computation shows that $f(\zeta_{10}) = 1 - \zeta_{10}$ implies $f(-1) \equiv 2 \pmod 5$, which is impossible since $f(-1)$ must be a unit in $Z[\zeta_2]$. It follows therefore that $\lambda_{10}(U_{10}) = \lambda_{10}(\overline{U}_{10})$.

It remains to compute the kernel of $\lambda_{10}|U_{10}$. This is not difficult to do directly, using (4.3) again, since we know the units of $Z[\zeta_5]$. We shall omit the computation here. The result is that the kernel is generated by $-\{x^5\}$ and $\{1 - x^2 - x^3 - x^7 - x^8\}$; it maps isomorphically onto the subgroup of $Z[\zeta_5]$ generated by -1 and $\zeta_5(1 + \zeta_5)^3$. The rank of U_{10} is 2, by Theorem (4.1), and the assertion of (d) now follows at once.

This completes the proof of Theorem (5.9).

Remark 5.22. Kummer has shown [7] that the second factor h_2 of the class number of $Q(\zeta_q)$ is not always equal to one for prime q. In particular, for $q = 163$, h_2 is divisible by 2; for $q = 229$ and $q = 257$, h_2 is divisible by 3. Since the order of $U_q/\overline{U}_q$ is given by h_2 for prime q, we see that, even for prime q, $\overline{U}_q$ is sometimes a proper subgroup of U_q. Furthermore, any $u \epsilon U_q$ with $A(u) = s$ can be written as $u = ve_s$ with $A(v) = 1$; hence we have also that $\overline{U}_q^1$ is a proper subgroup of U_q^1 for those values of q for which $h_2 \neq 1$.

§6. INDUCED AUTOMORPHISMS OF π_1 AND ORDERS OF SELF-EQUIVALENCES.

We shall summarize here in Theorem (6.2) some detailed information concerning the orders of elements of $\mathscr{E}(P_q)$. First we need to note a particular subgroup of $\mathscr{E}(P_q)$.

(6.1) *The dihedral subgroup* $\mathscr{D}(P_q)$. The space P_q is formed from the unit disk by the identification $(1, \theta) \equiv \left(1, \theta + \frac{2\pi}{q}\right)$; see the introduction. The rotation $(r, \theta) \to \left(r, \theta - \frac{2\pi}{q}\right)$ of the disk gives rise then to a homeomorphism $g: P_q \to P_q$ of order q which induces the identity on π_1. Also the reflection $(r, \theta) \to (r, -\theta)$ of the disk gives rise to a homeomorphism $g': P_q \to P_q$ such that $g'_*(a) = a^{-1}$. The group generated by g and g' is abstractly just the dihedral group of order $2q$; indeed, replacing the disk by a polygon of q sides, it is clearly the group of homeomorphisms of P_q arising from the rigid symmetries of the polygon.

Let us denote by $\mathscr{D}(P_q)$ the subgroup of $\mathscr{E}(P_q)$ generated by $\{g\}$ and $\{g'\}$. It is easy to compute that $\gamma_g = \{x\}$ and $\gamma_{g'} = -1$ in E_q (see definitions 1.8 and 3.2); hence the κ of Theorem (3.4) maps $\mathscr{D}(P_q)$ isomorphically onto the dihedral subgroup of E_q consisting of the trivial elements $\pm\{x^k\}$.

THEOREM 6.2. *For* $s \epsilon Z_q^*$, *let* $\mathscr{E}^s(P_q)$ *denote the subset of* $\mathscr{E}(P_q)$ *consisting of all* $\{f\}$ *for which* $f_*(a) = a^s$. *Then* $\mathscr{E}^1(P_q)$ *is an abelian normal subgroup of* $\mathscr{E}(P_q)$, *whose rank is the number of integers between* 1 *and* $q/2$ *which do not divide* q, *and the* $\mathscr{E}^s(P_q)$ *are its* $\phi(q)$ *distinct cosets.*

(a) *The elements of finite order in the subgroup* $\mathscr{E}^1(P_q) \cup \mathscr{E}^{-1}(P_q)$ *are precisely the elements of the dihedral subgroup* $\mathscr{D}(P_q)$ *of* (6.1).

(b) *If* $s \neq \pm 1$, $\mathscr{E}^s(P_q)$ *contains infinitely many elements whose order is equal to the order of* s.

(c) *If* s *is primitive* (i.e. *has order* $\phi(q)$), *every element of* $\mathscr{E}^s(P_q)$ *has order* $\phi(q)$.

(d) *If* s *is semi-primitive but not primitive, every element of* $\mathscr{E}^s(P_q)$ *has order a multiple of* $\frac{1}{2}\phi(q)$; *this multiple may be* 1 *or* 3 *for* q *odd and* 1, 2, 3, 4 *or* 6 *for* q *even; see Remark* 6.11 *below.*

(e) *If* s *is not semi-primitive,* $\mathscr{E}^s(P_q)$ *contains infinitely many elements whose order is infinite.*

For the proof of this theorem we need the two lemmas which follow; they are also of some interest in their own right; see Remarks (6.10), (6.11) and (7.1).

LEMMA 6.3. *For any* $u \epsilon U_q$, $\theta_{-1}(u) = \{x^{2j}\}u$ *for some* j.

Proof. Let $v = u^{-1}\theta_{-1}(u)$, We consider the projection onto the summand $Z[\zeta_h]$ in (4.3):

$$\lambda_h : \Gamma_q \to Z[\zeta_h] \qquad h|q,\ h \neq 1 \tag{6.4}$$

and set $z_h^{(s)} = \lambda_h \theta_s(v)$. Note that the numbers $z_h^{(s)}$, for all $s \epsilon Z_q^*$, include $\lambda_h(v)$ and all its conjugates in $Z[\zeta_h]$. But

$$z_h^{(s)} = (\lambda_h \theta_s(u))^{-1}(\lambda_h \theta_{-1}\theta_s(u)) = (\lambda_h \theta_s(u))^{-1}\overline{(\lambda_h \theta_s(u))} \tag{6.5}$$

where the bar denotes complex conjugate. Hence $|z_h^{(s)}| = 1$, all s, from which it follows that $\lambda_h(v)$ is a root of unity; see [16, p. 705].

Using the monomorphism (4.3) now, since $\lambda_h(v)$ has finite order for each h on the right it follows that v has finite order and, therefore, by Theorem (4.1), $v = \pm\{x^m\}$ for some m. Clearly $A(v) = 1$ so that $v = +\{x^m\}$. If q is odd, there always exists a j such that $m \equiv 2j$

(mod q) and then $v = \{x^{2j}\}$. If q is even, $\lambda_2(v) = (\lambda_2(u))^2 = +1$ clearly; but $\lambda_2(v) = (-1)^m$, so that m must be even. This completes the proof.

We introduce next a notion closely related to that of the "norm" in algebraic number theory.

Definition 6.6. Given $\gamma \epsilon \Gamma_q$ and $s \epsilon Z_q^*$, we set

$$N(\gamma) = \prod_{t \epsilon Z_q^*} \theta_t(\gamma), \qquad N_s(\gamma) = \prod_{m=0}^{k-1} \theta_{s^m}(\gamma)$$

where k = order of s.

LEMMA 6.7. *Let u be in U_q and let $2j$ be as in Lemma* (6.3). *Let s be in Z_q^* and set $\sigma(s) = 1 + s + \cdots + s^{k-1}$* (mod q) *where k = order of s.*

(a) $N(u) = 1$ *so that, if s is primitive,* $N_s(u) = 1$.

(b) *If s is semi-primitive,* $(N_s(u))^2 = \{x^{-2j\sigma(s)}\}$.

(c) *For all* $s \epsilon Z_q^*$

$$N_s\left\{\frac{1 - x^{s^{i+1}}}{1 - x^{s^i}}\right\} = 1, \qquad \text{all } i.$$

(d) *If $t \epsilon Z_q^*$ and $t \neq \pm s^m$ for all m, then*

$$N_s\left\{\frac{1 - x^{t^{i+1}}}{1 - x^{t^i}}\right\}$$

has infinite order in U_q for all i.

Proof (a). Let λ_h be as in (6.4), with $h|q$, and let $N(\lambda_h u)$ denote the norm of $\lambda_h u$ in the usual sense; see [16, p. 558]. Then it is clear that $\lambda_h N(u) = (N(\lambda_h u))^m$ where m is the order of the kernel of the epimorphism $Z_q^* \to Z_h^*$. Now $N(\lambda_h u)$ is a rational integer and a unit and is, therefore, ± 1. But $\lambda_h \theta_t(u)$ and $\lambda_h \theta_{-t}(u)$ are a complex conjugate pair so that $\lambda_h N(u)$ is positive. Thus $\lambda_h N(u) = 1$ for all $h|q$. Since the λ of (4.3) is a monomorphism, it follows that $N(u) = 1$.

(b) If s is semi-primitive, $N_s(u)\,\theta_{-1}(N_s(u)) = N(u) = 1$, by part (a). Since $\theta_{-1}\theta_s = \theta_s\theta_{-1}$, we get from Lemma (6.3) that $\theta_{-1}N_s(u) = \{x^{2j\sigma(s)}\}N_s(u)$ and (b) follows at once.

(c) Let $\eta_j = \{(1 - x^{s^{j+1}})/(1 - x^{s^j})\}$ for all j; clearly $\eta_{j+k} = \eta_j$. Then $N_s(\eta_i) = \eta_i\eta_{i+1} \cdots \eta_{i+k-1} = \eta_0\eta_1 \cdots \eta_{k-1}$ and this is clearly 1.

(d) Let $v = \{(1 - x^{t^{i+1}})/(1 - x^{t^i})\}$ and suppose $(N_s(v))^n = 1$. Let $h(\neq 1)$ divide q and let ζ_h be a primitive h-th root of unity; set $\mu_m = 1 - \zeta_h^{c_m}$ where $0 < c_m < q/2$ and $c_m \equiv \pm s^m t^{i+1}$ (mod q); set $v_m = 1 - \zeta_h^{d_m}$ where $0 < d_m < q/2$ and $d_m \equiv \pm s^m t^i$ (mod q). Since $(1 - \zeta_h^w)^{2q} = (1 - \zeta_h^{-w})^{2q}$ for all $w \epsilon Z$, we get

$$1 = (\lambda_h N_s(v))^{2qn} = \mu_0^{2qn}\mu_1^{2qn} \cdots \mu_{k-1}^{2qn} v_0^{-2qn} v_1^{-2qn} \cdots v_{k-1}^{-2qn} \tag{6.8}$$

where k = order of s. It follows from the hypothesis that $c_m \neq d_{m'}$ for all m, m' (although $c_m = c_{m'}$ and $d_m = d_{m'}$ are possible). Since (6.8) holds for all h dividing q ($h \neq 1$), the theorem quoted in (5.20) above requires that $n = 0$. This completes the proof of the lemma.

Proof of Theorem 6.2. Let E_q be as in Definition (3.2) and let E_q^s consist of those $\gamma \epsilon E_q$ for which $A(\gamma) = s$; in particular, then, $E_q^1 = U_q^1$. It is clear that the isomorphism κ of

Theorem (3.4) maps $\mathscr{E}^s(P_q)$ onto E_q^s. In proving Theorem (6.2) then we may replace $\mathscr{E}^s(P_q) \subset \mathscr{E}(P_q)$ everywhere by $E_q^s \subset E_q$.

The first part of the theorem then follows at once from Theorem (3.5) and Corollary (4.3).

For (a)–(e), let us choose a particular element v_s in each E_q^s such that the order of $v_s = k$ = order of s; we can do this by Theorem (3.5). In particular, we take $v_1 = +1$, $v_{-1} = -1$ Then any element of E_q^s can be written uniquely in the form $u \circ v_s$ where $u \epsilon E_q^1 = U_q^1$ and $\circ$ denotes the multiplication in E_q; see (3.2). Clearly, from (3.2) and (6.6),

$$(u \circ v_s)^k = N_s(u) \qquad \text{in } U_q^1 \tag{6.9}$$

and the order of $u \circ v_s$ is k times the order of $N_s(u)$ in U_q^1.

For (a) then, $N_1(u) = u$ and $N_{-1}(u) = \{x^{2j}\}u^2$ by Lemma (6.3). By Corollary (4.3), $u \epsilon U_q^1$ has finite order if and only if $u = \{x^m\}$ for some m. Thus only the elements $\pm \{x^m\}$ have finite order in $E_q^1 \cup E_q^{-1}$ and this, with (6.1), proves (a).

Part (b) follows from (c) of Lemma (6.7), using $u = \{(1 - x^{s^{i+1}})/(1 - x^{s^i})\}^{kn}$ for any $n \epsilon Z$; since $s \neq \pm 1$, this u is never trivial, by Corollary (4.3).

Part (e) follows similarly from (d) of Lemma (6.7) and part (c) is immediate from (a) of that lemma.

Finally, for part (d), let ω be the additive order of $\sigma(s)$ in Z_q, where $\sigma(s)$ is as in Lemma (6.7). It is clear that, for $d \epsilon Z_q^*$, if $d \equiv s^m$ for some m, then $\omega | d - 1$ and if $d \equiv -s^m$ for some m, then $\omega | d + 1$. Now, for q odd, $2 \epsilon Z_q^*$; hence $\omega = 1$ or 3. But for q odd and $u \epsilon U_q^1$, (b) of Lemma (6.7) gives us $N_s(u) = \{x^{-j\sigma(s)}\}$ and it follows that $N_s(u)$ has order 1 or 3.

For q even, by the same argument, if $3 \epsilon Z_q^*$, $\omega | 2$ or $\omega | 4$; if $5 \epsilon Z_q^*$, $\omega | 4$ or $\omega | 6$. If neither 3 nor 5 is in Z_q^*, then, by Definition (5.3), both 7 and 11 are in Z_q^* and it follows that $\omega | 4$ or $\omega | 6$. In all cases then, either $\omega | 4$ or $\omega | 6$. Applying this to (b) of Lemma (6.7) we get that either $N_s(u)^4 = 1$ or $N_s(u)^6 = 1$.

This completes the proof of Theorem (6.2).

Remark 6.10. In the proofs of Lemmas (6.3) and (6.7) we have used the fact that $\lambda_h \theta_{-1}(u) = \overline{\lambda_h(u)}$, where λ_h is as in (6.4). In view of this we might call $\theta_{-1}(u)$ the "complex conjugate" of u and define u to be "real" if $\theta_{-1}(u) = u$. It follows from Lemma (6.3) that for each $u \epsilon U_q$ there is an $\{x^j\}$ such that $\{x^j\}u$ is real; if q is odd, this j is unique.

Looking now at U_q^1, we can denote by R_q^1 the subgroup of elements invariant under θ_{-1}, i.e. the "real" subgroup of U_q^1; let T_q^1 denote the torsion subgroup of U_q^1, generated by $\{x\}$. For odd q, R_q^1 is free and we can write U_q^1 canonically as a direct product $U_q^1 = T_q^1 \times R_q^1$ For even q, the torsion part of R_q^1 consists of 1, $\{x^{q/2}\}$; we can write U_q^1 now as the direct product of T_q^1 and a free subgroup of R_q^1 of index 2, but this latter is no longer canonically determined. Note that this explains the definition of b_i in (5.13).

Remark 6.11. The possible multiples indicated in (d) of Theorem (6.2), which are just the orders of the $N_s(u)$ of (6.9), all occur in particular cases. Thus, for $q = 9$, $s = 4$, $N_s\{x\}$ has order 3; for $q = 8$, $s = 5$, $N_s\{x\}$ has order 4; for $q = 18$, $s = 7$, $N_s(x)$ has order 6.

In general, however, much more precise estimates of order for Theorem (6.2(d)) are possible using the formula of Lemma (6.7(b)). For example, if $\{f_0\}\epsilon\mathcal{E}^s(P_q)$ has order $\frac{1}{2}\phi(q)$, then an element $\{ff_0\}\epsilon\mathcal{E}^s(P_q)$ for which γ_f is "real" (see (6.10)) has order $\frac{1}{2}\phi(q)$ for odd q and either $\frac{1}{2}\phi(q)$ or $\phi(q)$ for even q.

§7. VARIOUS REMARKS

The present section is devoted to some brief notes relevant to our general problem.

(7.1). *Free homotopies.* Let g and g' be as in (6.1). The map $g^k: P_q \to P_q$ is homotopic to the identity by a homotopy which moves the base point through a loop representing $a^k\epsilon\pi_1$. Letting $\mathcal{F}(P_q)$ denote the group of *free* self-equivalence classes (i.e. in the sense of free homotopy), and using (6.1) and Theorem (3.4), it follows at once that $\mathcal{F}(P_q)$ is isomorphic to E_q/T_q^1, where T_q^1 is the cyclic group generated by $\{x\}$. Theorem (3.5) gives us then a split extension:

$$1 \to \frac{U_q^1}{T_q^1} \xrightarrow{i} \frac{E_q}{T_q^1} \xrightarrow{A} Z_q^* \to 1 \tag{7.2}$$

where i and A are as before. Note that U_q^1/T_q^1 may be replaced here by the "real" subgroup R_q^1 of U_q^1 for q odd, and by a free subgroup of R_q^1 of index 2 for q even; see Remark (6.10). Since U_q^1/T_q^1 is free, some of the earlier considerations (e.g. Theorem (6.2.)) become a little simpler for $\mathcal{F}(P_q)$.

Note also that, by Lemma (6.3), the dihedral subgroup D_q consisting of the elements $\pm\{x^k\}$ is normal in E_q. Using (6.1) then, $\mathcal{E}(P_q)/\mathcal{D}(P_q)$ is isomorphic to E_q/D_q and once again we get a split extension

$$1 \to \frac{U_q^1}{T_q^1} \xrightarrow{i} \frac{E_q}{D_q} \xrightarrow{A} \frac{Z_q^*}{(1,-1)} \to 1 \tag{7.3}$$

which we could study algebraically.

(7.4). *Lens spaces and their self-equivalences.* If a 3-dimensional lens space $L = L(q: m)$ is given in the usual cellular subdivision, then P_q is its 2-skeleton. It is natural in the context of the present work to ask for the group $\mathcal{E}(L)$.

The answer turns out to be very simple. By [11, §8] we see (assuming $q > 2$) that there is exactly one self-equivalence class inducing the automorphism $a \to a^s$ of $\pi_1(L)$ if $s^2 \equiv \pm 1 \pmod q$, and none at all if $s^2 \not\equiv \pm 1 \pmod q$. Thus the group $\mathcal{E}(L)$ is isomorphic to the subgroup of Z_q^* consisting of those elements whose square is ± 1. (For $q = 2$, $\mathcal{E}(L) \approx Z_2$.)

(7.5). *Construction of self-equivalences corresponding to given elements of E_q.* It should be noted that the correspondence κ of Theorem (3.4) is completely effective in the inverse direction also; i.e. given $\gamma\epsilon E_q$ we can construct explicitly a corresponding self-equivalence f, as follows. We let $p(x)$ be a polynomial in $Z[x]$ representing γ, with $0 < p(1) < q$, and let $w(x) = (p(x) - p(1))/(1 - x)$. Let $\alpha_0\epsilon\pi_2(P_q)$ be chosen as indicated for Lemma (2.11) and set $\alpha = w(a)\alpha_0$. Finally, let f_s be the special map defined in §2 above (following (2.3)) for $s = p(1)$. We then construct f by "altering" f_s on the cell σ_2 of our triangulation of P_q by the homotopy element α. This is a standard procedure (see [10, (1.8)]) which leaves f_s

unchanged except in the interior of σ_2 and gives an f such that $\mathcal{C}^2(f, f_s)$ is represented by the cocycle $\alpha\sigma^2$. It follows from Corollary (2.13) and Theorem (3.4) then that $\kappa\{f\}$ is the given γ.

(7.6). *Induced automorphisms of* $\pi_2(P_q)$. It is of some interest to know the automorphism f_* of $\pi_2(P_q)$ induced by a self-equivalence f or, more particularly, the connection between this automorphism and γ_f. Using (2.10), we have

$$f_*(\alpha_0) = \eta_f \alpha_0 \tag{7.7}$$

for some $\eta_f \epsilon \Gamma_q$, and f_* is completely determined by this η_f and the automorphism $a \to a^s$ of π_1 induced by f.

It is not difficult to prove the analogue of Corollary (2.13) for η_f. We omit the proof and give simply the result, namely that with f and η as in Corollary (2.13),

$$\eta_f = \{s(1 + a + \cdots + a^{s-1})\} + \{1 - a^s\}\eta. \tag{7.8}$$

Eliminating η, this gives us the desired relation

$$\eta_f = \{1 + a + \cdots + a^{s-1}\}\gamma_f. \tag{7.9}$$

We could have studied the self-equivalence group by means of the invariant η_f instead of γ_f, but the results do not come out quite so neatly. Since $A(\eta_f) = s^2$, η_f determines s^2, but not s, and there are always two different elements of $\mathcal{E}(P_q)$ corresponding to the same η_f, one sending $a \to a^s$, the other $a \to a^{-s}$. Thus γ_f determines η_f, but not conversely unless s is also given.

§8. APPENDIX: A RELATION BETWEEN OBSTRUCTIONS AND INDUCED HOMOMORPHISMS OF COHOMOLOGY

We shall prove here (Corollary (8.8)) a more general version of Lemma (2.9).

We suppose given a locally finite simplicial pair (X, A), an arbitrary pathwise connected space Y and a map $f: A \to Y$ which is extendable to $X^n \cup A$ (i.e. to the n-skeleton of X) so as to induce a specified homomorphism $\theta: \pi_1(X; *) \to \pi_1(Y, *)$. Let $\pi_n = \pi_n(Y, *)$, let G be any local group at $*$ in Y and suppose given $y \epsilon H^n(Y; G)$. Let $\theta^*\pi_n$ and θ^*G be the corresponding local groups in X induced by θ from π_n and G in Y. Let $\mathcal{O}_\theta^{n+1}(f)$ be the $(n+1)$-st obstruction to an extension of f which induces θ. Our purpose is to give a formula which shows how $\mathcal{O}_\theta^{n+1}(f) \subset H^{n+1}(X, A; \theta^*\pi_n)$ determines $\delta f^* y \epsilon H^{n+1}(X, A; \theta^*G)$.

For this purpose we define a homomorphism

$$y_\square : \pi_n(Y, *) \to G \tag{8.1}$$

by the same procedure as we used for (2.7). That is, given $\alpha \epsilon \pi_n$, we take $\phi: (S^n, *) \to (Y, *)$ representing it and define $y_\square(\alpha) = (\phi^* y)(h_n)$, where h_n is the generator of $H_n(S^n; Z)$ given by the orientation of S^n. (If G is a simple coefficient system, then $y_\square$ is just the Hurewicz homomorphism $\pi_n \to H_n(Y; Z)$ composed with the element of $Hom(H_n(Y, Z); G)$ determined by y.)

It is clear that $y_\square$ is a homomorphism of local groups and therefore may be regarded also as a homomorphism of local groups in X:

$$y_\square : \theta^*\pi_n \to \theta^*G \tag{8.2}$$

and consequently induces

$$y_* : H^k(X, A; \theta^*\pi_n) \to H^k(X, A; \theta^*G). \tag{8.3}$$

We have then the following formula:

PROPOSITION 8.4 $$\delta f^* y = y_* \mathcal{O}_\theta^{n+1}(f).$$

Proof. We may suppose without loss of generality that f maps all vertices of A to $*$ in Y. Let F be any extension of f to $X^n \cup A$ inducing θ and also mapping all vertices to $*$. We suppose the vertices of X ordered and let σ be any $n+1$-simplex, which we may regard also as a singular simplex of X.

If $c^{n+1}(F)$ denotes the obstruction cocycle determined by F, then $(c^{n+1}(F)(\sigma))$ is the element of π_n defined by $F|\dot{\sigma}$, where $\dot{\sigma}$ is the oriented boundary of σ. It follows from (8.1) then that

$$y_\square(c^{n+1}(F)(\sigma)) = (\phi^* y)(h_n) \tag{8.5}$$

where $\phi = F|\dot{\sigma}$ and $h_n \epsilon H_n(\dot{\sigma}; Z)$ is represented by the cocycle $\sum (-1)^i \sigma^{(i)}$. If z is a singular cocycle representing y and $F^\#$ denotes the induced cochain map, the right hand side of (8.5) is given by

$$(\phi^* y)(h_n) = \omega \cdot (F^\# z)(\sigma^{(0)}) + \sum_{i=1}^{n+1} (-1)^i (F^\# z)(\sigma^{(i)}) \tag{8.6}$$

where ω is the element of $\pi_1(Y, *)$ defined by F restricted to the leading edge of σ. Thus,

$$y_\square(c^{n+1}(F)(\sigma)) = (\delta F^\# z)(\sigma) \tag{8.7}$$

and the proposition follows at once.

The corresponding result for homotopies is then an obvious corollary. Given $f, g: X \to Y$ with $f|A = g|A$ and $f \cong g$ rel A in dimension $n-1$, we get immediately from Proposition (8.4) (see [12, p. 25 and p. 31]).

COROLLARY 8.8. $(f-g)^* y = y_*(\mathcal{O}^n(f, g) \text{ rel } A)$.

Lemma (2.9) is just a special case of this result. The general formula given in Corollary (8.8) is an extremely useful one in studying problems of homotopy and homology classification of mappings.

REFERENCES

1. M. ARKOWITZ and C. R. CURJEL: The group of homotopy equivalences of a space, *Bull. Amer. Math. Soc.* **70** (1964), 293–296.
2. W. D. BARCUS and M. G. BARRATT: On the homotopy classification of the extensions of a fixed map, *Trans. Amer. Math. Soc.* **88** (1958), 57–74.
3. H. CARTAN and S. EILENBERG: *Homological Algebra*, Princeton University Press, 1956.
4. W. FRANZ: Über die Torsion einer Überdeckung, *J. reine angew. Math.* **173** (1935), 245–254.
5. K. IWASAWA: A class number formula for cyclotomic fields, *Ann. Math., Princeton* **76** (1962), 171–179.
6. E. E. KUMMER: Sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers, *J. math. pures appl.* **16** (1851), 377–498.
7. E. E. KUMMER: Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen und über den zweiten Faktor der Klassenzahl, *Mber. Dtsch Akad. Wissenschaften, Berlin* (1870), 855–880.
8. H. B. MANN: *Introduction to Algebraic Number Theory*, Ohio State University Press, 1955.

9. H. MINKOWSKI: Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen, *J. reine angew Math.* **107** (1891), 278–297.
10. P. OLUM: Obstructions to extensions and homotopies, *Ann. Math., Princeton* **52** (1950), 1–50.
11. P. OLUM: Mappings of manifolds and the notion of degree, *Ann. Math., Princeton* **58** (1953), 458–480.
12. P. OLUM: Invariants for effective homotopy classification and extension of mappings, *Mem. Amer. Math. Soc. No. 37*, 1961.
13. W. SHIH: On the group $\mathscr{E}[X]$ of homotopy equivalence maps, *Bull. Amer. Math. Soc.* **70** (1964), 361–365.
14. H. S. VANDIVER: Fermat's last theorem, *Amer. Math. Mon.* **53** (1946), 555–578.
15. I. M. VINOGRADOV: *Elements of Number Theory*, Dover, New York, 1954.
16. H. WEBER: *Lehrbuch der Algebra*, vol. II, third ed., Chelsea, London.
17. E. WEISS: *Algebraic Number Theory*, McGraw-Hill, New York, 1963.
18. P. WOLFSKEHL: Beweis, dass der zweite Factor der Klassenzahl für die aus den elften und dreizehnten Einheitswurzeln gebildeten Zahlen gleich Eins ist, *J. reine angew. Math.* **99** (1886), 173–178.

Cornell University,
Ithaca, New York